FORM **NCSS-1**
(4/24/06)

OMB No. 1121-0301: Approval Expires 08/31/2008

2005 NATIONAL COMPUTER SECURITY SURVEY

RETURN COMPLETED FORM TO:
RAND Corporation
Survey Research Group
1776 Main Street
P.O. Box 2138
Santa Monica, CA 90407-2138

OR
FAX TO:
1-877-814-6673

For assistance
Phone: 1-800-734-5399
Monday through Friday
8:00 a.m. to 5:00 p.m. Pacific Time
OR
E-mail: ncss@rand.org

NOTICE OF CONFIDENTIALITY—Your report is confidential by law (P.L. 107-347, Title V and 44 U.S.C. § 3501 note). It may be seen only by persons certified to uphold the confidentiality of information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that your responses are immune from legal process.

U.S. DEPARTMENT OF JUSTICE
BUREAU OF JUSTICE STATISTICS

In partnership with the

U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL CYBER SECURITY DIVISION

SURVEY SCOPE
This voluntary survey collects data on the type and frequency of computer security incidents in which a computer was used as the means of committing a crime against the company.

REPORTING ENTITY
Report consolidated figures for DOMESTIC OPERATIONS of this company, including all DIVISIONS and LOCATIONS, and **excluding** SUBSIDIARIES. *Use figures that include subsidiaries only if figures excluding subsidiaries are not available.* For this survey, subsidiary means a company in which this company has more than 50% ownership, or in which this company has the power to direct or cause the direction of management and policies.

REPORTING PERIOD
The reporting period for this survey is CALENDAR YEAR 2005. If 2005 calendar year figures are not available, please use fiscal year 2005 data.

ESTIMATES
If exact figures are not available, estimates are acceptable.

Use a dark colored pen to fill out the survey. Completely fill in the squares ■ or circles ● to indicate your responses. To indicate an answer selected in error, draw a heavy "X" over the square or circle. When reporting a number, avoid writing on the edge of the response box. Please refer to the instructions on page 14 before completing the survey.

I. COMPUTER SECURITY CONCERNS

1a. What are the top three computer security concerns for this company? *Mark ■ up to three.*

- ☐ Computer virus, worm, or Trojan horse
- ☐ Denial of service
- ☐ Electronic vandalism or sabotage
- ☐ Embezzlement
- ☐ Fraud
- ☐ Theft of intellectual property (copyrights, patents, trade secrets, trademarks)
- ☐ Unlicensed use or copying (piracy) of digital products—software, music, motion pictures, etc.—developed for resale
- ☐ Theft of personal or financial information such as names and dates of birth; social security numbers; credit/debit/ATM card, account, or PIN numbers; etc.
- ☐ Other computer security incidents such as hacking, spoofing, phishing, sniffing, pinging, scanning, spyware, adware, other malware, etc.
- ☐ Misuse of computers by employees (Internet, e-mail, etc.)
- ☐ Breaches resulting from information obtained from stolen laptops
- ☐ Other → Specify: _____

b. What three potential sources of computer security threat are of greatest concern to this company? *Mark ■ up to three.*

- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Domestic competitor
- ☐ Foreign competitor
- ☐ Domestic hacker
- ☐ Foreign hacker
- ☐ Other → Specify: _____

II. COMPUTER INFRASTRUCTURE & SECURITY

2a. In 2005, what types of computer networks (including Internet) or equipment did this company use?
For this survey, "company" means DOMESTIC OPERATIONS, including all DIVISIONS and LOCATIONS. *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptops
- ☐ Laptops not owned by company
- ☐ Other → Specify: _____

b. In 2005, what types of network access did this company support? *Mark ■ all that apply.*

- ☐ Hard-wired telecommunications lines
- ☐ Remote dial-in access via telecommunications lines
- ☐ Access to company networks or e-mail through Internet
- ☐ Wireless access to e-mail
- ☐ Wireless access to Internet
- ☐ Wireless access to this company's data or other networks
- ☐ Publicly accessible website WITHOUT e-commerce capabilities
- ☐ Publicly accessible website WITH e-commerce capabilities
- ☐ Other → Specify: _____

II. COMPUTER INFRASTRUCTURE & SECURITY - Continued

3a. In 2005, what types of computer system security technology did this company use? *Mark ■ all that apply.*

- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators (smartcards, tokens, keys)
- ☐ Passwords that must be changed periodically
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ E-mail logs or filters
- ☐ System administrative logs
- ☐ Encryption
- ☐ Other → Specify: _____

b. In 2005, how much did this company spend on the types of computer system security technology identified in 3a?
ESTIMATES are acceptable.
EXCLUDE personnel costs.

	Mil.			Thou.			Dol.		
$							0	0	0

c. What percentage of this company's total 2005 Information Technology budget did this company spend on the types of computer system security technology identified in 3a?
ESTIMATES are acceptable.
Round to nearest whole percent.

			%

d. What types of computer system security technology does this company plan to add in 2006?
EXCLUDE updates or upgrades of technologies already used in 2005.
Mark ■ all that apply.

- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators (smartcards, tokens, keys)
- ☐ Passwords that must be changed periodically
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ E-mail logs or filters
- ☐ System administrative logs
- ☐ Encryption
- ☐ Other → Specify: _____
- ☐ Do not plan to add any new technologies in 2006

4a. In 2005, what types of computer security practices did this company have? *Mark ■ all that apply.*

- ☐ Business continuity plan for computer systems
- ☐ Disaster recovery plan for computer systems
- ☐ Corporate policy on computer security
- ☐ Identification of company's critical assets
- ☐ Vulnerability/risk assessment
- ☐ Intrusion/penetration testing of computer security
- ☐ Computer/network watch center
- ☐ Configuration management
- ☐ Regular review of system/security administration logs
- ☐ Periodic computer security audits
- ☐ Formal computer security audit standards
- ☐ Physical/environmental security (e.g., limited physical access, sprinklers)
- ☐ Personnel policies (e.g., background checks, transfer, termination)
- ☐ Training employees in computer security practices
- ☐ Equipment decommissioning
- ☐ Other → Specify: _____

b. In 2005, what computer security functions did this company outsource? INCLUDE fully and/or partially outsourced functions.
Mark ■ all that apply.

- ☐ Business continuity plan for computer systems
- ☐ Disaster recovery plan for computer systems
- ☐ Corporate policy on computer security
- ☐ Identification of company's critical assets
- ☐ Vulnerability/risk assessment
- ☐ Intrusion/penetration testing of computer security
- ☐ Computer/network watch center
- ☐ Configuration management
- ☐ Regular review of system/security administration logs
- ☐ Periodic computer security audits
- ☐ Formal computer security audit standards
- ☐ Physical/environmental security (e.g., limited physical access, sprinklers)
- ☐ Personnel policies (e.g., background checks, transfer, termination)
- ☐ Training employees in computer security practices
- ☐ Equipment decommissioning
- ☐ Other → Specify: _____
- ☐ None; all computer security was done in-house

c. If this company had a computer system business continuity or disaster recovery plan, was it tested, used in an emergency situation and/or updated in 2005?
Mark ■ all that apply.

- ☐ Tested in 2005
- ☐ Used in emergency situation in 2005
- ☐ Updated in 2005
- ☐ Had plans but did not test, use, or update in 2005
- ☐ Other → Specify: _____
- ☐ Not applicable; did not have these plans in 2005

d. In 2005, how frequently did this company conduct formal vulnerability/risk assessments prior to implementing new applications, systems, or programs? *Mark ■ all that apply.*

- ☐ Always
- ☐ More than half the time
- ☐ Less than half the time
- ☐ When required by law
- ☐ Other → Specify: _____
- ☐ Never
- ☐ Did not implement any new applications, systems, or programs in 2005.

e. In 2005, did this company track downtime caused by any computer security incidents?

- ○ Yes
- ○ No

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS

The questions in this section pertain to computer security incidents against this company, where the word "incident" refers to any unauthorized access, intrusion, breach, compromise or use of this company's computer system.

Computer security incidents may be committed by people either inside or outside the company and include computer virus, denial of service, vandalism, sabotage, embezzlement, fraud, theft of intellectual property, theft of personal or financial information, or other incidents such as hacking, spoofing, or spyware.

Please do NOT duplicate information. If an incident can be classified under multiple categories, report it under the FIRST applicable category. For example, if part of the company's computer system was deliberately damaged by means of a virus, report this under computer virus, not vandalism or sabotage.

ESTIMATES are acceptable.

5. COMPUTER VIRUS

A computer virus is a hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

INCLUDE viruses, worms, Trojan horses, etc.

EXCLUDE spyware, adware, other malware, etc. Report these in 12 (Other Computer Security Incidents) on page 11.

a. In 2005, did this company intercept any computer viruses before they could infect any part of its computer systems?

- ◯ Yes
- ◯ No
- ◯ Don't know

b. Did this company detect any viruses which infected any part of its computer systems in 2005?

- ◯ Yes → **How many incidents were detected?** *If a virus simultaneously infects a server and one or more PCs, count this as ONE INCIDENT.* ☐☐☐☐☐☐ Number
- ◯ No → **(If "No", skip to 6.)**

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-Virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Through which of the following were the viruses introduced into this company's networks in these incidents? *Mark ■ all that apply.*

- ☐ E-mail attachments
- ☐ Software installation
- ☐ Files brought in on portable media such as floppy disks, CDs, or flash drives
- ☐ Files downloaded from the Internet
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 5e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations specified in 5e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

h. What was the relationship between the suspected offender (the person who sent or created the virus) and this company at the time of the incidents indicated in 5b? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. What was the total downtime (in hours) for each of the following due to these virus infections? ESTIMATES are acceptable.

INCLUDE downtime needed for repair.

1. Downtime of servers, routers or switches Hours | | | | | | |

2. Downtime of individual PCs/workstations Hours | | | | | | |
EXCLUDE network downtime reported above in item i,1.

j. How much was spent in 2005 to recover from these computer viruses? ESTIMATES are acceptable.

INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc.
EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.			Thou.			Dol.
$							0 0 0

k. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable.

INCLUDE actual losses such as the value of lost information.
INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.			Thou.			Dol.
$							0 0 0

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

6. DENIAL OF SERVICE

Denial of service is the disruption, degradation, or exhaustion of an Internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, excessive amounts of incoming data, etc.

EXCLUDE incidents already reported under 5 (Computer Virus) on page 3.

a. Did this company detect any incidents of denial of service (a noticeable interruption of its Internet connection or e-mail service) in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 7.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 6d? ☐☐☐☐☐☐ Number

f. If any incidents were not reported to the organizations specified in 6d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 6a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the total duration (in hours) of the incidents of denial of service indicated in 6a? ESTIMATES are acceptable. INCLUDE downtime needed for repairs. Hours ☐☐☐☐☐☐

i. How much was spent in 2005 to recover from these incidents of denial of service? ESTIMATES are acceptable. INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

7. ELECTRONIC VANDALISM OR SABOTAGE

Electronic vandalism or sabotage is the deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, programs, etc.

EXCLUDE incidents already reported under 5 (Computer Virus) on page 3.

EXCLUDE incidents of alteration which resulted in fraud. Report these in 9 (Fraud) on page 8.

a. Did this company detect any incidents in which files, data, web pages or any part of its computer systems were electronically vandalized or sabotaged in 2005?

○ Yes → **How many incidents were detected?** Number

○ No → **(If "No", skip to 8.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 7d? Number

f. If any incidents were not reported to the organizations listed in 7d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 7a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the total downtime (in hours) of each of the following due to these acts of vandalism or sabotage? ESTIMATES are acceptable.

INCLUDE downtime needed for repair.

1. Downtime of company websites/ web servers	Hours
2. Downtime of servers, routers or switches EXCLUDE downtime reported above in item h,1.	Hours
3. Downtime of individual PCs/workstations EXCLUDE downtime reported above in item h,1 or 2.	Hours

i. How much was spent in 2005 to recover from these incidents of vandalism or sabotage? ESTIMATES are acceptable. INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE actual losses such as the value of lost information. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
$			000

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

8. EMBEZZLEMENT

Embezzlement is the unlawful misappropriation of money or other things of value, BY THE PERSON TO WHOM IT WAS ENTRUSTED (typically an employee), for his/her own use or purpose.

INCLUDE instances in which a computer was used to wrongfully transfer, counterfeit, forge or gain access to money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by the person to whom it was entrusted.

a. Did this company detect any incidents in which a computer was used to commit embezzlement against this company in 2005?

○ Yes → **How many incidents were detected?** [ ][ ][ ][ ][ ][ ] Number

○ No → **(If "No", skip to 9.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following official organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 8d? [ ][ ][ ][ ][ ][ ] Number

f. If any incidents were not reported to the organizations specified in 8d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 8a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the dollar value of money or other things taken by embezzlement in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$	[ ][ ][ ]	[ ][ ][ ]	000

i. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable.
INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.
EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$	[ ][ ][ ]	[ ][ ][ ]	000

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

9. FRAUD

Fraud is the intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

INCLUDE instances in which a computer was used by someone inside or outside this company in order to defraud this company of money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by means of forgery, misrepresented identity, credit card or wire fraud, etc.

EXCLUDE incidents of embezzlement. Report these in 8 (Embezzlement) on page 7.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to commit fraud against this company in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 10.)**

b. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

c. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

d. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

e. How many of these incidents were reported to the organizations specified in 9d? ☐☐☐☐☐☐ Number

f. If any incidents were not reported to the organizations specified in 9d, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

g. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 9a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

h. What was the dollar value of money or other things taken by fraud in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$			000

i. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

10. THEFT OF INTELLECTUAL PROPERTY

Theft of intellectual property is the illegal obtaining of copyrighted or patented material, trade secrets, or trademarks including designs, plans, blueprints, codes, computer programs, software, formulas, recipes, graphics, etc., usually by electronic copying.

EXCLUDE incidents of theft of personal or financial data such as credit card or social security numbers, names and dates of birth, financial account information, etc. Report these in 11 (Theft of Personal or Financial Data) on page 10.

EXCLUDE incidents of theft of any other type of information. Report these in 12 (Other Computer Security Incidents) on page 11.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to obtain intellectual property from this company in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 11.)**

b. What type of intellectual property was obtained? *Mark ■ all that apply.*

- ☐ Copyrighted material
- ☐ Patented material
- ☐ Trade secrets
- ☐ Trademarks

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 10e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations specified in 10e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

h. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 10a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. What was the dollar value of intellectual property taken by theft in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$			000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

k. How many of the incidents indicated in 10a involved unlicensed use or copying (piracy) of digital products which this company developed for resale? ☐☐☐☐☐☐ Number

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

11. THEFT OF PERSONAL OR FINANCIAL INFORMATION

Theft of personal or financial information is the illegal obtaining of information that could potentially allow someone to use or create accounts under another name (individual, business, or some other entity). Personal information includes names, dates of birth, social security numbers, etc. Financial information includes credit/debit/ATM card, account, or PIN numbers, etc.

EXCLUDE incidents of theft of intellectual property such as copyrights, patents, trade secrets, and trademarks. Report these in 10 (Theft of Intellectual Property) on page 9.

EXCLUDE incidents of theft of any other type of information. Report these in 12 (Other Computer Security Incidents) on page 11.

a. Did this company detect any incidents in which someone inside or outside this company used a computer to obtain personal or financial information from this company in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 12.)**

b. What type of personal or financial information was obtained? *Mark ■ all that apply.*

- ☐ Names or dates of birth
- ☐ Social security numbers
- ☐ Credit card numbers
- ☐ Debit or ATM card numbers
- ☐ Account or PIN numbers
- ☐ Other → Specify: _____

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation) Emergency Readiness Team)
- ☐ US-CERT (United States Computer
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 11e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations specified in 11e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization →Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other →Specify: _____

h. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 11a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. What was the dollar value of personal or financial information taken by theft in 2005? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
$			000

j. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE the cost of diagnosis, repair and replacement such as labor, hardware, software, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$			000

13532

III. TYPES OF COMPUTER SECURITY INCIDENTS – Continued

12. OTHER COMPUTER SECURITY INCIDENTS

INCLUDE all other computer security incidents involving this company's computer networks—such as hacking, sniffing, spyware, theft of other information—regardless of whether damage or losses were sustained as a result.

EXCLUDE incidents already reported in this survey.

a. Did this company detect any other computer security incidents in 2005?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No → **(If "No", skip to 13.)**

b. What other types of computer security incidents were detected in 2005? *Mark ■ all that apply.*

- ☐ Hacking
- ☐ Spoofing
- ☐ Phishing
- ☐ Sniffing
- ☐ Pinging
- ☐ Scanning
- ☐ Spyware, keystroke logging
- ☐ Adware
- ☐ Other malware
- ☐ Theft of information not already reported in 10 or 11 on pages 8 or 9 → Please describe: _____
- ☐ Other → Please describe: _____

c. Which of the following types of security technology or practices were inadequate in preventing these incidents? *Mark ■ all that apply.*

- ☐ Internal computer security controls
- ☐ External computer security controls
- ☐ Anti-virus software
- ☐ Anti-spyware/adware software
- ☐ Biometrics
- ☐ One-time password generators
- ☐ Passwords that must be changed
- ☐ Digital certificates
- ☐ Firewall
- ☐ DMZ Host
- ☐ Intrusion Detection System
- ☐ Intrusion Protection System
- ☐ Encryption
- ☐ Software vulnerability/buffer overload
- ☐ E-mail filters or review of e-mail logs
- ☐ Review of system/security admin logs
- ☐ Computer network/watch center
- ☐ Configuration management
- ☐ Physical/environmental security
- ☐ Personnel policies
- ☐ Authorized access misused
- ☐ Other → Specify: _____
- ☐ Don't know

d. Which of the following were used, accessed, or affected in these incidents? *Mark ■ all that apply.*

- ☐ Local area network (LAN)
- ☐ Wide area network (WAN)
- ☐ Process control network (PCN)
- ☐ Virtual private network (VPN)
- ☐ Wireless network (e.g.,802.11)
- ☐ Electronic data interchange (EDI)
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Stand-alone PCs (not on LAN)
- ☐ Company-owned laptop
- ☐ Laptop not owned by company
- ☐ Other → Specify: _____
- ☐ Don't know

e. To which of the following organizations were these incidents reported? *Mark ■ all that apply.*

- ☐ Local law enforcement
- ☐ State law enforcement
- ☐ FBI (Federal Bureau of Investigation)
- ☐ US-CERT (United States Computer Emergency Readiness Team)
- ☐ Other Federal agency → Specify: _____
- ☐ CERT® Coordination Center
- ☐ ISAC (Information Sharing and Analysis Center)
- ☐ InfraGard
- ☐ None of the above

f. How many of these incidents were reported to the organizations specified in 12e? ☐☐☐☐☐☐ Number

g. If any incidents were not reported to the organizations listed in 12e, what were the reasons? *Mark ■ all that apply.*

- ☐ Handled internally
- ☐ Reported to third party contractor providing computer security services
- ☐ Reported to another organization → Specify: _____
- ☐ Negative publicity
- ☐ Lower customer/client/investor confidence
- ☐ Competitor advantage
- ☐ Did not want data/hardware seized as evidence
- ☐ Did not know who to contact
- ☐ Incident outside jurisdiction of law enforcement
- ☐ Did not think to report
- ☐ Nothing to be gained/nothing worth pursuing
- ☐ Other → Specify: _____

h. What was the relationship between the suspected offender and this company at the time of the incidents indicated in 12a? *Mark ■ all that apply.*

- ☐ Insider - someone currently (or formerly) working for this company
- ☐ Current employee
- ☐ Current contractor, vendor, temporary worker, etc.
- ☐ Former employee, contractor, vendor, temporary worker, etc.
- ☐ Outsider - someone who never worked for this company
- ☐ Domestic competitor
- ☐ Foreign competitor → Specify country: _____
- ☐ Domestic hacker
- ☐ Foreign hacker → Specify country: _____
- ☐ Other hacker (origin unknown)
- ☐ Other → Specify: _____
- ☐ Don't know

i. If any, what was the total downtime (in hours) of each of the following due to these other computer security incidents? ESTIMATES are acceptable.

INCLUDE downtime needed for repair.

1. Downtime of company websites/ web servers	Hours	☐☐☐☐☐☐
2. Downtime of servers, routers or switches EXCLUDE downtime reported above in item i,1.	Hours	☐☐☐☐☐☐
3. Downtime of individual PCs/workstations EXCLUDE downtime reported above in item i,1 or 2.	Hours	☐☐☐☐☐☐

j. How much was spent in 2005 to recover from these other computer security incidents? ESTIMATES are acceptable. INCLUDE the cost - both internal and external - of diagnosis, repair, and replacement such as labor, hardware, software, etc. EXCLUDE costs associated solely with the prevention of future incidents.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

k. What other monetary losses and costs were incurred in 2005 due to these incidents? ESTIMATES are acceptable. INCLUDE actual losses such as the value of lost information. INCLUDE the estimated value of downtime, lost productivity, income from lost sales, abor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	000

13532

IV. OTHER TRENDS IN COMPUTER SECURITY

13. In 2005, did this company detect any computer security breaches that resulted from information obtained from a stolen laptop computer?

○ Yes → **How many incidents were detected?** ☐☐☐☐☐☐ Number

○ No

14. In 2005, was the overall number of computer security incidents detected by this company more, less or about the same compared to the number detected in 2004 regardless of whether damage or losses were sustained as a result? *Mark ● only one.*

○ More in 2005

○ Less in 2005

○ About the same

○ Don't know

15. In 2005, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?

○ Yes

○ No

○ Don't know

16. In 2005, what percentage of this company's business was transacted over the Internet, Intranet, Extranet, EDI, etc.?
ESTIMATES are acceptable.
INCLUDE any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services. For example, taking orders for merchandise or services, transferring information or rights, paying accounts, etc. ☐☐☐ %

V. COMPANY INFORMATION

17. In 2005, which of the following Internet services, if any, did this company provide to other companies or individuals as its PRIMARY line of business? *Mark ■ all that apply.*

☐ Internet Service Provider (ISP)

☐ Web Search Portal

☐ Other Internet service →Specify: _____

☐ None of the above

18 a. What were the total operating revenue, sales, and/or receipts for this company in 2005?
ESTIMATES are

	Bil.	Mil.	Thou.	Dol.
$	☐☐☐	☐☐☐	☐☐☐	000

b. What percentage of this total was derived from e-commerce?
ESTIMATES are acceptable.
INCLUDE any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services. For example, taking orders for merchandise or services, transferring information or rights, paying accounts, etc. ☐☐☐ %

19. What was the total number of employees on this company's payroll for the pay period which includes March 12, 2005?
ESTIMATES are acceptable. *Count EACH part-time employee as one.* ☐☐☐☐☐☐☐☐ Number
EXCLUDE contractors, vendors, leased and temporary employees.

20. Does the information reported in this survey cover calendar year 2005, fiscal year 2005 or some other time period?

○ Calendar year 2005

○ Fiscal year 2005 or some other time period →Specify period covered:

FROM: ☐☐ ☐☐☐☐ (Month Year) TO: ☐☐ ☐☐☐☐ (Month Year)

21. Does the information reported in this survey include this company or does it include this company and some or all of its subsidiaries?
For this survey, subsidiary means a company in which this company has more than 50% ownership, or in which this company has the power to direct or cause the direction of management and policies.

○ Information includes this company only - company has no subsidiaries, or responses exclude subsidiaries

○ Information includes this company and some or all of its subsidiaries - **How many subsidiaries were included?** ☐☐☐ Number

13532

(Tear off sheet - identifying information will be separated from survey responses upon receipt by RAND.)

CONTACT INFORMATION

Person to contact regarding this report:

Name

Title

Company Name

Phone ( ) - Ext.

Fax ( ) -

E-mail address

Please list subsidiaries included in this report:

REMARKS

(Please use this space or a separate sheet of paper for any explanations that may be essential in understanding your reported data.)

13532

U.S. DEPARTMENT OF JUSTICE
BUREAU OF JUSTICE STATISTICS
In partnership with the
U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL CYBER SECURITY DIVISION

2005 NATIONAL COMPUTER SECURITY SURVEY INSTRUCTIONS

PURPOSE OF THE SURVEY

The purpose of this survey is to collect information about the nature and extent of computer security incidents experienced by businesses located in the U.S. The data you report will provide information on the impact of computer crime on businesses.

Specifically, data from the 2005 National Computer Security Survey will provide information on the frequency and types of crime involving computers, the monetary losses sustained as a result of computer crime, and the cost of computer security.

LEGAL AUTHORITY AND CONFIDENTIALITY

Your report is confidential by law (P.L. 107-347, Title V and 44 U.S.C. § 3501 note). It may be seen only by persons certified to uphold the confidentiality of this information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that your responses are immune from legal process.

BURDEN HOUR ESTIMATE

Respondents are not required to respond to any information collection unless it displays a valid approval number from the Office of Management and Budget. Public reporting burden for this collection of information is estimated to vary from 45 minutes to 3 hours per response, with an average of 1½ hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Bureau of Justice Statistics, National Computer Security Survey, Washington, DC 20531; and to the Office of Management and Budget, OMB No. 1121-0301, Washington, DC 20503.

GENERAL INSTRUCTIONS

Survey Scope – This survey collects computer security data for companies, organizations and associations operating within the United States. **Information for business-related activities of religious organizations, nonprofit organizations and organizations that are government owned but privately operated should be included.**

Reporting Entity – Report computer security data for all **domestic operations** of your company, including all divisions and locations. A company is a business, service or membership organization consisting of one or more establishments under common ownership or control**. Do not report for subsidiary companies that your company may hold, as they may be surveyed separately.** For this survey, subsidiary means a company in which this company has more than 50% ownership, or in which this company has the power to direct or cause the direction of management and policies. *Use figures that include subsidiaries only if figures that exclude subsidiaries are not available.* For purposes of this survey, exclude data for Puerto Rico, the Virgin Islands and U.S. Territories. If you are unable to consolidate records for the entire company minus subsidiaries or have reporting questions, please call **1–800–734-5399.**

How to Report Dollar Figures – Dollar figures should be **rounded** to thousands of dollars.

For example, if the figure is $1,023,528.79, enter:

Mil.	Thou.	Dol.
$ 1	0 2 4	

If the figure is less than $500.00, enter:

Mil.	Thou.	Dol.
$	0	

Estimates are acceptable – The data requested on the National Computer Security Survey may not correspond to your company's records. If you cannot answer a question from your company records, please provide a carefully prepared estimate.

Reporting Period – Report data for calendar year 2005. If you cannot provide data on a calendar year basis, fiscal year 2005 data are acceptable. If this company was not in operation for the full year, report for the period of time it was in operation. Indicate in Question 20, Report Period, the exact dates the data represent if they are not for the calendar year.

Additional Forms – Photocopies of this form are acceptable. If you require additional forms, contact us at the toll-free number, e-mail address, or business address provided below.

Filing the Report Form – Return your completed form in the pre-addressed envelope. If you are not using the pre-addressed envelope, return it to the address provided at the bottom of this page or fax it to 1–877-814-6673.

RAND Corporation
Survey Research Group
1776 Main Street
P.O. Box 2138
Santa Monica, CA 90407-2138

Direct any **QUESTIONS** regarding this form to:

Toll-free Number: 1-800-734-5399
FAX Number: 1-877-814-6673
E-mail: ncss@rand.org

GLOSSARY OF TERMS

Adware – A software application that automatically displays advertisements, typically in the form of pop-up windows. Adware sometimes includes spyware.

Anti-spyware/adware software – A utility that looks for spyware and/or adware and alerts the user to any that are found.

Anti-virus software – A utility that looks for viruses and alerts the user to any that are found.

Biometrics – Methods of generating authentication information for a person by digitizing measurements of a physical characteristic, such as a fingerprint, a hand shape, a retinal pattern, a speech pattern (voice print), or handwriting.

Business continuity plan for computer systems – The procedure an organization uses to maintain essential functions during and after a disaster, such as a dual back-up system at a separate physical location. It seeks to ensure the uninterrupted provision of mission-critical functions. It often includes a disaster recovery plan.

Company laptops – Any laptop computer issued by this company, whether owned or leased.

Computer/network watch center – The location from which control is exercised over a communications network, usually either telephony or Internet, though sometimes also that of a public utility. It is sometimes also the location containing many or all of the primary servers and other equipment that runs an internet service provider. This center is also where the technicians that maintain the servers, develop new software, and troubleshoot outages are located.

Configuration management – The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test fixtures, and test documentation of an automated information system, throughout the development and operational life of a system. Includes Source Code Management or revision control. The control of changes—including the recording thereof—that are made to the hardware, software, firmware, and documentation throughout the system lifecycle.

Corporate policy on computer security – A defined set of practices and guidelines established by the organization to deal with issues involving computer security. Such practices and guidelines can encompass the responsibilities of both the organization and its employees. Employees have been made aware of this policy.

Digital certificates – An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Disaster recovery plan for computer systems – A procedure to restore an organization's mission-critical functions after, and to minimize the effects of, a major interruption of computer services. It includes procedures for reporting specific types of problems to designated personnel, repairing or replacing damaged systems, etc.

DMZ Host – A small network that acts as a "neutral zone" between a company's internal network and an external network such as the Internet. A DMZ host is usually inserted behind or between firewalls.

Electronic Data Interchange (EDI) – A proprietary electronic system used for exchanging business data over a computer network.

E-mail logs or filters – E-mail logs keep track of incoming/outgoing messages, including the sender and the recipient. Filters are an automated method of searching the content of e-mail for words, viruses, or misuse of computer resources.

Encryption – The translation of data into a format that requires a code to restore it to the original format. To read an encrypted file, you must have access to a secret key or password that allows you to decrypt it.

Equipment decommissioning – A procedure used for removing computer equipment from active use within an information system or network. This involves changing settings within the system to reflect their absence, and the removal of all sensitive information from the computer equipment, particularly from hard drives and other media.

External computer security controls – Hardware, software, and/or company policies and practices limiting the access of outsiders to the company's computer systems and networks.

Extranet – A network that uses Internet/Intranet technology to make information available to authorized outsiders. It allows businesses to securely share information with selected suppliers, partners, customers, or other businesses.

Firewall – Hardware and/or software designed to prevent unauthorized access to or from a private network, particularly networks with Internet or Intranet connectivity.

Formal computer security audit standards – An established or authoritative set of criteria used to review computer security systems.

Hacker – An unauthorized person who cracks a computer system or exceeds authorized access for malicious intent or for the thrill of the challenge.

Hard-wired telecommunication lines – Telecommunication lines that are copper or fiber-optic and stationary, as opposed to wireless.

Identification of company's critical assets – Determining the critical functions that the organization performs, and the assets (such as information and telecommunication systems) upon which those functions are vitally dependent. Those critical assets are ones for which special security and reliability measures should be focused.

Insurance covering computer security breaches – This type of insurance specifically covers losses due to computer break-in exposures, usually in a separate policy or rider. The coverage is typically called network security liability, e-commerce liability, Internet security liability, or hacker insurance.

Internal computer security controls – Hardware, software, and/or company policies and practices limiting the access of insiders—employees, contractors, vendors, etc.—to the company's computer systems or networks. These controls may vary by department and/or employee function.

Internet – Inter-connected networks linking millions of computers globally. Users can access information and applications from other computers and communicate with other users.

Intranet – An internal network similar to the Internet but surrounded by a firewall to prevent access from users outside the company, organization, or facility.

Intrusion detection system – An intrusion detection system examines all inbound and outbound network activity and identifies suspicious patterns that may signal a network or system attack from someone attempting to break into or compromise a system.

Intrusion/penetration testing of computer security – A method of evaluating the security of a computer system and identifying its vulnerabilities by attempting to circumvent or override system security through the simulation of an attack by a malicious actor.

Intrusion protection system – A suite of access control tools used to protect computers from exploitation. Intrusion protection systems may also act at the host level to deny potentially malicious activity.

Local area network (LAN) – A computer network that spans a small area such as a single building or group of buildings.

Malware – Malicious software or code developed to serve a harmful purpose. Specific types of malware include viruses, worms, Trojan horses, spyware, and adware.

Misuse of computers by employees (Internet, e-mail, etc.) – The improper use of company computer resources by employees, such as using the company's computer resources for personal gain, sending personal or improper e-mail, abusing Internet privileges, loading unlicensed software, etc.

Non-company laptop – Any laptop computer not issued by this company (e.g., belonging to a consultant, vendor, contractor, etc.).

One-time password generators (smart cards, tokens, keys) – A "one-time password generator" is an authentication device such as a one-time token which randomly changes all or part of the user's password, typically every minute, so that the same password is never used more than once. This technique counters the threat of a replay attack that uses passwords captured by spyware, wiretapping, or other means of hacking.

Passwords that must be changed periodically – A simple authentication technique in which each password is used repeatedly for a specific period of time to verify an identity.

Periodic computer security audits – Reviews conducted periodically by the company's security office. For example, the company's strike team might simulate computer security situations and then evaluate how the company performed.

Phishing – The creation and use of fraudulent but legitimate-looking e-mails and web sites to obtain users' personal and financial account information for criminal purposes.

Physical/environmental security (e.g., limited physical access, sprinklers) – Security measures focused on limiting physical access to critical organization assets, and protection of those assets from physical malicious attacks (e.g., explosions) or natural disasters (earthquakes, fire, flood).

Pinging – A basic test of whether a particular host is operating properly and is reachable on the network from the testing host by sending a special packet of information and awaiting its response. Malicious use includes flooding the Internet with ping requests attempting to locate new hosts to infect, causing problems to routers across the Internet.

Piracy – see Unlicensed use or copying.

Process control network (PCN) – A network with an automated control of a process, such as a manufacturing process or assembly line. It is used extensively in industrial operations, such as oil refining, chemical processing, and electrical generation. It uses analog devices to monitor real-world signals and digital computers to do the analysis and controlling. It makes extensive use of analog/digital, digital/analog conversion.

Publicly accessible website WITH e-commerce capabilities – E-commerce capabilities refer to the ability of this company's customers or suppliers to effect transactions via computer networks. Such transactions commit the company and the customer/supplier to an exchange, though they do not necessarily include making payment associated with the commitment. For example, if a customer orders products via a website with payment made by check at a later date, this is an e-commerce transaction.

Regular review of system administrative logs – Reviewing system administrative logs on a regular basis to detect suspicious activity beyond normal daily activity.

Remote dial-in access – Refers to using devices and other resources that are not connected directly to a workstation to connect to another computer device. Do not include network access through the Internet.

Scanning – A method of searching for open ports by sending packets or requests for information.

Server – A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. A print server is a computer that manages one or more printers. A network server is a computer that manages network traffic.

Sniffing – Packet sniffing is a form of wire-tap applied to computer networks instead of phone networks. Traffic on a network segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus see everyone's traffic.

Spoofing – The creation of TCP/IP packets using someone else's IP address. A "spoofed" IP address is therefore misleading regarding the true source of an Internet message packet.

Spyware – Software that surreptitiously monitors the user and transmits the information to a third party. Some spyware can intercept or take partial control of a computer's operation. Spyware differs from viruses and worms in that it does not usually self-replicate.

Stand-alone PCs (not on LAN) – Computers that are not connected to company networks, such as a stand-alone workstation. For the purposes of this survey, a stand-alone computer may have Internet access.

System administrative logs – Logs which document details of access to computer systems, such as who logged in, which parts of the system were accessed, and when the user logged in and out.

Training employees in computer security practices – Training session(s) designed to educate employees on issues dealing with computer security and the employee's role in following the organization's computer security practices.

Trojan horse – A program that overtly does one thing while covertly doing another.

Unlicensed use or copying (piracy) of digital products developed for resale – The unauthorized copying or use of digital products — such as software, music, or motion pictures — which the company developed or for which it holds the copyright. Report unauthorized copying or use of other software by employees under "Misuse of computers by employees (Internet, e-mail, etc.)."

Virtual private network (VPN) – A network that is constructed by using public wires to connect nodes. For example, systems that allow you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network.

Virus – A hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

Vulnerability/risk assessment – Assessment of threats to, impacts on, and vulnerabilities of information and information-processing facilities and the likelihood of their occurrence.

Wide area network (WAN) – A computer network that spans a large geographical area. Usually, a WAN consists of two or more LANs.

Wireless networks (e.g., 802.11) – A type of LAN that uses high-frequency radio waves or lasers rather than wires to communicate between nodes. 802.11 refers to a family of specifications for an over-the-air interface between a wireless client and a base station or between two wireless clients.

Wireless access to e-mail, Internet and/or this company's other networks – Wireless access refers to the use of a device or system that will enable access to a network to which it is not physically connected. For example, access via a cellular or digital phone, some personal digital assistants (PDAs), some laptop computers, thin client, broadband, etc.

Worm – A self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.